ESCC
Enterprise Solutions Competency Center

U.S. ARMY ENTERPRISE SOLUTIONS COMPETENCY CENTER

Federated Identity Management (FIdM) Reference Guide

In Partnership with the U.S. Navy

Introduction

The Army and Navy recently signed a data-sharing memorandum of understanding. As an extension of the newly signed agreement and shared data environment, the decision was made to jointly produce a reference guide addressing the many facets of identity management that directly rely on shared data and trust.

The purpose of this reference guide is threefold:

- To provide a high-level overview of identity management
- To promote discussion that will generate policies defining the boundaries of identity management
- To define a common language for identity management and federated identity management.

Identity management is critical to becoming net-centric, and without addressing both the technical and non-technical aspects it will fail. Biometrics, access control, architectures, infrastructure, and the traditional aspects of identity management are much more clearly defined than policy, governance, education, and social/personal implications. Through critical thinking and shared goals, true identity management can be achieved in the effort to support the global war on terror.

Identity management is the combination of systems, rules, and procedures that define an agreement between an individual and an organization(s) regarding ownership, utilization, and safeguarding of personal identity information and all collateral information, explicit and inferable, associated with that identity.

> *“However beautiful the strategy, you should occasionally look at the results.”*
> — Winston Churchill

Evolution of Identity Management

Pre-Information Age (1960 – 1980)

- Limited computing resources available
- Data tracked, collected, and secured manually

Information Age (1980 – 2000)

- Start of automated data processing
- Silos of incompatible systems, networks, and software
- World Wide Web was born

Open Standard for Web Services (1998 – 2004)

- Large software corporations collaborate to define standards
- Consensus on a single set of standards is exclusive

Federation Age (2004 – present)

- Identity theft becomes a household word
- The speed of commercial transactions and volume of information exchange creates information overload and an informational generation gap

ESCC Key Concept

The Internet was begun in the mid-1960s as a military command and control systems research project. The original network was known as DARPAnet and expanded in the early 1970s to include government and research institutions.

Identity Federation

The ultimate goal of an identity federation is to enable users of one domain to securely access data, systems, or applications of another domain seamlessly and without the need for completely redundant user administration.

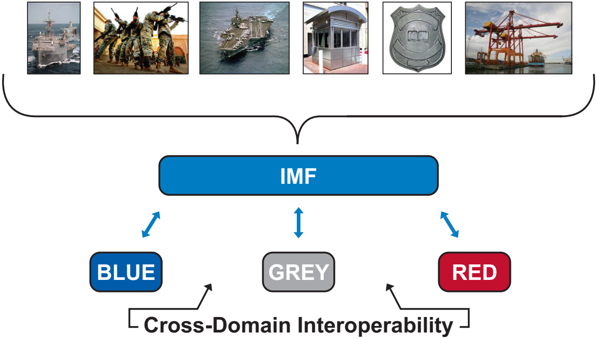
- Dissimilar business units become enabled to conduct business activities independently from other business units while sharing information at their own discretion.
- Federations are predicated on trust.
- Within identity management, an identity federation allows individuals or organizations to use root identities to interact with the world across a broad range of applications.
- Examples include:
  - Law enforcement, national security, health, access control, communications, transactions, identity protection, immigration, transportation, voting, human resources, etc.

IdM Objectives – Modeled

☑ Applications

☑ Information Sharing

☑ Root ID



IMF

BLUE

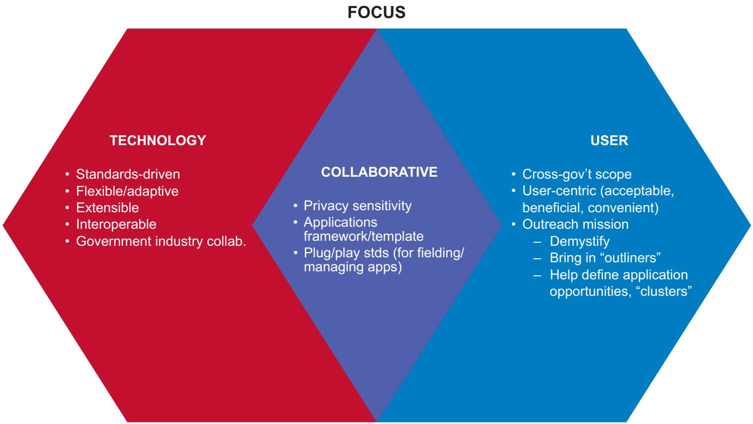
GREY

RED

Cross-Domain Interoperability

Identity Management Continuum

Comprehensive Approach to IdM



FOCUS

TECHNOLOGY

- Standards-driven
- Flexible/adaptive
- Extensible
- Interoperable
- Government industry collab.

COLLABORATIVE

- Privacy sensitivity
- Applications framework/template
- Plug/play stds (for fielding/ managing apps)

USER

- Cross-gov't scope
- User-centric (acceptable, beneficial, convenient)
- Outreach mission
  - Demystify
  - Bring in "outliners"
  - Help define application opportunities, "clusters"

National Security

Federal Biometrics:

One person, one identity

- Border control:
  - Enforce immigration policies
- Law enforcement:
  - First responders enabled in times of national emergency
- Coalition/international partners:
  - Solidify and define data-sharing relationships
- Interagency information sharing:
  - Improve communication
  - Validate credentials and location
- Improved identity protection

ESCC Key Concept

Identity federation is a key enabler for net-centric warfare. The user's credentials serve as "tags" — so "tagged data" can be accordingly filtered, sanitized, searched, and shared according to the producer's criteria.

Value of Federated Identity

Operations and Logistics

- **Attain accurate characterization** – Identifies red, blue, and gray forces. Detects objects in the battle space, which allows for the assignment of threat levels and role-based access and privileges.

- **Reduced administration** – User administration occurs only at the "home domain."

- **Instantaneous access** – Warfighters and emergency responders get instant access to information required to provide role-based functions, which enables overall mission functionality.

- **Cross-domain information sharing** – Because access is granted on an individual basis and access control decisions are made before information is shared, segregated networks are not necessary.

- **Better control of what gets shared** – Allows more specific, rule-based access control; user activities are logged; users must authenticate their identities.

Eliminates Inefficiencies and Risk

- Eliminates unauthorized use of systems after termination of user(s)
- Reduces fraud (client and provider) — eliminates duplication of identification
- Improves service and social welfare conditions (eliminates card sharing, phantom services, etc.)
- Achieves policy outcomes (ties use of IdM to policy)
- Mitigates risk — 66% of surveyed employees report keeping paper password records

Overview:
Take a long-term, strategic view of the FIdM enterprise, systems integration at representative domains, and the access control policy for different data types. FIdM is inherently scalable — so use pilot projects liberally — especially when exploring access control rules.

- **Develop policies and governance** – Today, governance and convention issues are the most challenging. Create policies that will scale as the use of identity expands (from simple access to portals to Service Oriented Architecture orchestration and attribute-based filters). FIdM is a key enabler to net-centric operations — because it “tags” users based on their credentials. FIdM can be applied to portals, Web sites, military software applications, collaborative tools, even voice networks.

- **Use pilot projects** – IAM technology enables a new way of doing business. Small pilot projects are useful in defining the access control policy that will help define and explore the boundaries of governance.

- **Scalability** – The scope of a federation is relative to every organization. While some organizations deal with sister military organizations, others must federate with coalition partners, civil government, and even commercial organizations. Each organization can use FIdM to create their own access control policies to deal with their own relative enterprises.

- **Strategic steps** – Because FIdM is truly net-enabled and is a key enabler to other net-enabled foundation elements (advertise data, only handle information once, etc.) — plan the doctrinal and workflow advances in increments to support IdM collection, processing, analysis, decision making, and action.

External Considerations of Identity

- **Privacy** – A user's personal information may be shared with partner organizations that may store the data or otherwise use it in an unauthorized manner.

- **Anonymity** – Some users may require anonymity to carry out their duties or prefer a degree of anonymity while working with federation partners.

- **Release ability** – Users want control of what information is released to outside agencies. Technology allows user information to be collected from various sources and pieced together without the user's knowledge.

ESCC Key Concept

The claims that are presented to a service provider can be tailored for each federation partner. Many identity systems allow the user to specify which attributes are shared.

Key Organizational Requirements

- Governance between organizations:
  - Form agreements to use pseudo information
  - Develop acceptable use policies

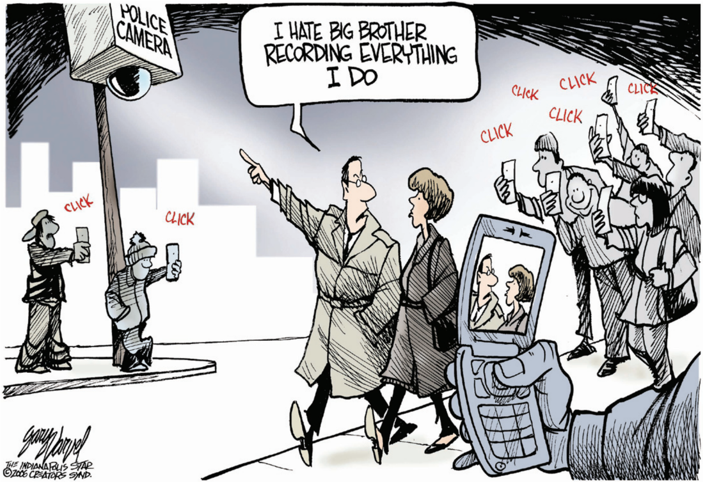
- Information sharing:
  - Provide only enough information to the federated partner to make an access control decision
  - Allow users to stipulate what information is presented to a partner
  - Allow users to approve the sending of information that is in an assertion
  - Use translucent databases (databases that only allow the user to unlock certain data)
  - Minimize use of personally identifiable information (PII) on smart cards
  - Store PII in personnel management systems — allows more selective release, is more authoritative, is difficult to replicate
  - Use pseudo information such as names or aliases for approved data transformation (e.g. only use last four digits of a user’s Social Security number)

Key Organizational Challenges

- Maintain federated trust (multi-service/Defense/interagency/international):
  - Personnel within each domain must be self-policing and adhere to federation agreements
- Articulate access control policy to ensure the right information is shared with only the right people:
  - Red force
  - Blue force
  - Neutral
- Information assurance and information technology must work together to convert the access control policy into access control rules that the FIdM system can enforce:
  - Biometrics
  - Credentials
  - Contextual data
  - Forensics
  - Verification and identification

ESCC Key Concept

The claims that are presented to a service provider can be tailored for each federation partner. Many identity systems allow the user to specify which attributes are shared.



(Reprinted with permission of Gary Varvel and Creators Syndicate, Inc.)

Myth: The government ("big brother") was the driving force behind the use of identity management and FIdM.

Fact: Banks, e-commerce, the transportation industry, and communications companies are examples of industry leaders being the first to explore federated identity management concepts beginning around the year 2000. The U.S. government didn't engage until after 9/11 by passing Homeland Security Presidential Directive 12 (HSPD-12) in 2001 and Sarbannes Oxley in 2002.

ESCC Key Concept

HSPD-12 is a mandate for the method by which smart cards are issued, programmed with user data, and transmitted without contact using data transmission. The Department of Defense Common Access Card implementation preceded the HSPD-12 directive and is not in compliance.

Myth: FIdM is an all-or-nothing proposition with regards to data sharing.

Fact: FIdM is a different way of doing business from segregated networks. Role-based access controls allow for shades of gray admissions to data. Users have access only to that information for which they have specific privileges and authorizations. For example, an intelligence officer will have access to different levels and types of personnel data than an infantry officer, who, in turn, will have different levels and types of access than a physician at a combat surgical hospital.

Myth: Policy and governance that define and regulate identity management are widely used, easily accessible, and cover all aspects of identity management.

Fact: Policy and governance for identity management are not clearly defined. There are many social, legal, and political aspects that remain unaddressed at a national level. At a minimum, participants in a federated environment must agree to:

- Make valid assertions regarding the entities they are affirming — including the user's authentication instance
- Enforce the safeguarding of shared information
- Perform audits — both logical (i.e. data logs) and physical (physical security) — de-provision unauthorized users, use data protection policies.

Myth: The federated enterprise is less secure than segregated networks.

Fact: While the only guaranteed method for preventing intrusion is physical segregation of domains, the components of FIdM (authentication, encryption, access control) provide greater encryption capability and allow the data provider better risk mitigation tools than are currently in place by leveraging rule-based access controls.

ESCC Key Concept

The use of a demarcation zone (DMZ) network segment is essential to providing security to the internal security domain. The DMZ is a segment that provides a tightly controlled zone for information sharing. If there is unacceptable risk to sharing a piece of data, don't copy it into the DMZ.

Top 10 Misconceptions

Myth: Every domain in the federated enterprise must purchase identical hardware.

Fact: Hardware and software solutions that adhere to open standards are designed to be compatible. How those standards are implemented must be addressed — either between partners or as a condition of joining a federation — to ensure system interoperability of data and services.

ESCC Key Concept

Military and paramilitary (public safety, first responder) relationships are usually formed based on an individual's assignment within an organization.

Myth: Every user across the federated enterprise must authenticate in the same manner.

Fact: While multifactor authentication provides better assurance that users are who they say they are, the decision to grant access to information can be based on the authentication method. This sliding scale of trust is useful when dealing with partners that do not use smart cards or biometrics and in emergency or combat situations where these authentication methods are impractical.

ESCC Key Concept

Start by trusting the IdP; then, as the infrastructure matures, inspect the authentication event information; finally, challenge the IdP or ask for additional credentials when an access control decision is pending.

Top 10 Misconceptions

Myth: The Biometrics Program, for which the Army is the executive agency, covers all aspects of Department of Defense identity management.

Fact: Biometrics are measurable physical characteristics or personal behavioral traits used to recognize the identity, or verify the claimed identity, of an individual. Biometrics does not address global identity management that supports voluntary and involuntary subjects, U.S. and non-U.S. persons, or privacy data and public perceptions.

ESCC Key Concept

Federated partners can allow similar access to resources with increased flexibility and immediate de-provisioning and without the information technology overhead and coordination complications.

Myth: Identity management applies only to back-end business operations.

Fact: Identity management technology includes:

- Combat identification
- Force protection
- Detention operations
- Personnel recovery and identification
- Civil-military operations
- Medical processes
- Financial transactions

ESCC Key Concept

The tamperproof smart card has two key pairs, one for encryption, and one for identification. The private key is never released to the network. Department of Defense refers to its implementation as the Common Access Card.

Top 10 Misconceptions

Myth: Federation partners access high-assurance (classified) networks directly.

Fact: Sensitive data is moved from a high-assurance classified network to a demarcation zone (DMZ) network assignment. Shared information should be moved in and out of the DMZ through pre-approved technical specifications. The federation partner doesn't access high-assurance networks directly.

Myth: Identity management infrastructure will replace the existing investment.

Fact: The most significant augmentation to the existing infrastructure is the addition of an identity provider (that provides an assertion vouching for the user) and the service provider (SP). The SP accepts the assertion, makes an access control decision, and subsequently provides the information. Most access control products integrate with existing Web host applications — there may little need to buy a new Web host.

ESCC Key Concept

The major investment is in re-engineering the access control systems. Governance and establishing technical conventions between federation partners are the two biggest hurdles — not the technology.

Criteria for Success

- The enterprise has adopted the view that information superiority is a warfighting multiplier, and against an unconventional adversary, the enterprise of knowledge is a weapon.

- Technology allows the data to be shared between any two partners and only governance and use policies prescribe order and discretion.

- Access controls are carefully crafted to allow information security and adequate permeability to maximize end-user effectiveness.

- There are mutually agreed upon definitions and applications for both hard science (technical) and social science (based on law and intuition).

- Unwillingness of the information assurance community to allow change
- Lack of policy and governance
- Unavailability of core enterprise services or incorrect use for promoting adoption of net-centric transformation
- Lack of cooperation or collaboration between operational authority (who gets access to what) and information technology (IT) community (implementing access control)
- Inadequate addressing of technical governance issues that establish trust
- Inadequate articulation of conventions that allow dissimilar business units to convey identity
- Lack of adherence of independent business units to federation governance
- Insufficient funding
- Lack of IT skills within the organization

Reasons for Failure

Critical Success Factors (CSFs)

CSF #1: Clearly Defined Business Processes

- Sharing agreements have been executed
- Partnership roles defined
- Business responsibilities agreed upon

CSF #2: Solutions to Liability Issues

- All partners agree that benefits outweigh risks
- Partners agree to work through the issues

CSF #3: Visible Audit Processes

- Help mitigate risk
- User activities tracked for inappropriate behavior
- Behavior used to detect intrusion

CSF #4: Defined Privacy Boundaries

- Necessary user credentials defined for access control decisions
- Decisions made about when/if the information will be stored

CSF #5: Credentialing Policies Implemented

- Decide how user credentials will be:
  - Verified
  - Suspended
  - Revoked

CSF #6: Clear Technical Conventions

- Common syntax and semantics agreed upon
- Protocols established within the identity framework
- Mutual agreement about how credentials will be issued

Critical Success Factors (CSFs)

Mitigating Strategies

Independent inspectors ensure that federation partners comply with:

- Governance
- Standards
- Conventions

Federation partners collaborate to inspect audit logs to:

- Detect intrusion
- Identify inappropriate behavior
- Take corrective action immediately
- Improve user efficiency

Create demarcation zones (DMZs) to protect unshared data and establish a zone where information is selectively shared:

- Data should only move between the classified segment and the DMZ through filtering and sanitizing systems
- There may be more than one DMZ for a sensitive domain.

Establish the data producer’s access control policy (rules) to limit who gets access to what:

- Rule-based access control
- Role-based access control
- Proximity-based access control
- Billet-based access control.

Mitigating Strategies

Control Methods

Logical Access

- **Role-based access control** – Access control decisions are based on a user's role within his or her organization.

- **Rule-based access control** – Access control decisions are based on a set of rules that supplement, but may include, role, proximity, or billet. These rules help mitigate risk by stipulating the conditions for information sharing such as: IP ranges, MAC addresses, authentication requirements, time, or condition flags.

- **Proximity-based access control** – Access control decisions are based on an entity's (includes devices) reported location. In addition to mitigating risk, this is useful in bandwidth throttling and tailoring data views. These rules stipulate that the entity's location identifier matches a geocode (i.e. ZIP code, state abbreviation) or the reported position is within a polygon or volume.

- **Billet-based access control** – Similar to but more specific than rule-based access control, billet-based access control defines a specific duty position within an organization. For example, “surgeon” is a role and “chief of surgery” is the position. This distinction is useful in defining role-based communities of interest that may be used for alerting systems and collaborative tools and pre-planning information architectures.

ESCC Key Concept

Logical and physical access control systems are beginning to converge. Verifying the identity of individuals both within an organization and among different organizations has become critically important.

Control Methods

Physical Access

- **System operational components:**
  - PIV card
  - PIV card reader/keypad
  - Biometric reader
  - Control panel
  - Access control server
  - Cardholder data repository
  - Control points
- **Rights and privileges:**
  - Defined by local PACS manager who enrolls the PIV card's data
  - Possession of a PIV card does not automatically grant facility access
  - Each agency develops policies that govern how to accept and authenticate cardholders requiring facility access
  - Right to access facilities controlled locally or remotely
  - Remote control requires multiple facilities to be linked using an enterprise-level control system that shares information in a common database
  - Privileges can be denied using different methods (suspension to revocation)

- **Access control policy** – A set of rules used by the service provider, usually associated with a role or other dynamic attributes. It is normally used for access provisioning and access reconciliation. The access control device makes the decision to grant access by comparing the attributes made in the asserting claim regarding the identity with the access control policy.

- **Authentication** – Users' actions validate who they say they are. This is accomplished by proving:

  - What you know (password)
  - What you have (digital personal public key infrastructure certificate)
  - Who you are (fingerprint).

Multifactor authentication (i.e. certificate and PIN) may be required to provide stronger verification.

Biometrics – A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an individual. Facial images, fingerprints, and iris scan samples are all examples of biometrics.

Claims – An assertion made by a claimant of the value or values of one or more identity attributes of a digital subject.

Digital identity – A digital representation of a set of claims made by one digital subject about itself or another digital subject. The mediation of people's experience of their identities versus the identity of other people and things through the use of technology.

Demarcation zone (DMZ) – A network segment that is established for sharing data. This segment is insulated from a sensitive segment by approved guards, data-diodes, and firewalls. This logical zone carefully watches for intruders and inappropriate behavior.

Digital rights management (DRM) – The science of protecting data so that only the intended recipient can use it. Championed by the entertainment industry, this technology hinders a recipient from further sharing or otherwise using data inappropriately even if obtained legitimately. Today, there is still no guarantee that a partner cannot copy shared data.

Enrollment – The act of registering people into a defined environment with a defined set of boundaries.

Federation – A union of independent organizations (domains) that are all bound by agreements and communications technology and predicated on trust.

Federated trust – An instance of a relationship between two or more entities (domains) in which an entity assumes that another entity will act as authorized/expected. The risk/trust relationship depends on who you are and what you want to do at any instance. The degrees of separation (chain of custody) between parties can decrease the trust (increase the risk).

Federated policy – The rules, applied across all federation members, technically enabled by various intelligent actuation and measurement devices that enforce governance elements.

Governance – The overarching component of trust comprised of non-technical elements. These are the agreements (contracts, memorandums of understanding, acceptable use policies, etc.) that lay the legal foundation for forming a federation.

Identity management (ID management) – A broad administrative area that deals with uniquely identifying individuals in a system (such as a country, a network, or an enterprise) and controlling their access to resources within that system by associating user rights and restrictions with the established identity.

Identity theft – The illegal acquisition of the set of physical and behavioral characteristics by which an individual is uniquely recognizable.

Match – Authentication of a key aspect of trust-based identity attribute, providing a codified assurance of the identity of one entity to another. Examples of authentication methodologies include the presentation of a unique object, the provision of confidential information, or the confirmation of ownership of an e-mail address.

Modality – In human-computer interaction, a modality is the general class of:

- A sense through which the human can receive the output of the computer (for example, vision modality)
- A sensor or device through which the computer can receive the input from a human.

In less formal terms, a modality is a path of communication between a human and a computer.

One to many – A relationship that occurs when one entity is related to many occurrences in another entity. An act of publishing or broadcasting from one sender to many receivers.

One to one – A relationship that occurs when one entity is related to only one other entity. An act of publishing or broadcasting from one sender to one receiver.

Root identity – An identity that is transportable over time and distance and has been authenticated through uniquely verifiable identity enrollment. The enrollee must be able to assert a true identity in order to access resources or avoid sanctions.

Trust – An evaluation, by an entity, of the reliability of an identity when the identity is involved in interactions. The level of trust is typically based on the technical strength of the identity (including authentication method, authoritative attributes, physical security), but it also includes evaluating the entity's subjective considerations (e.g. feelings) of the reliability of the entity the identity represents.

Defense Science Board Report on Defense Biometrics, http://www.acq.osd.mil/dsb/reports/2007-03-Biometrics.pdf

Communications and Definition Resource, http://searchunifiedcommunications.techtarget.com/sDefinition/0,,sid186_gci906307,00.html

Industry Initiatives on Federated Identity Management, http://www.securitydocs.com/library/2782

Risks and Rewards of Federated Identity Management, http://www.networkcomputing.com/channels/security/showArticlejhtml?articleID=196901490

Linux in Government, http://www.linuxjournal.com/article/8431

Useful Web Sites

Benefits and Drawbacks of Federated Identity Management,
http://www.csoonline.com/read/100106/fea_federated_idm.html

Open Source Federated Identity Management,
http://www.sourceid.org/

Identity Management News and Resources,
http://www.networkworld.com/topics/identity-management.html

Windley, Phillip, “Hidden Challenges of Federated Identity,” InfoWorld, March 24, 2006

Simmons, Doug, “Identity Management Discussion Group,” Educause, August 10, 2004

Radcliff, Deborah, “Identity Management in the Real World,” CSO Magazine, November 2004

Petraborg, John; Scott, Diane, “Viewpoint Paper Social Welfare Identity Management: Building the Business Case for Public Investment,” EDS, January 17, 2008

Smart Card Alliance Physical Access Council White Paper, “FIPS 201 and Physical Access Control: An Overview of the Impact of FIPS 201 on Federal Physical Access Control Systems,” Publication Number: PAC-05001, September 2005

“Report of the Defense Science Board Task Force on Defense Biometrics,” Department of Defense, March 2007

www.wikipedia.com
www.dictionary.com

U.S. ARMY ENTERPRISE SOLUTIONS COMPETENCY CENTER

ESCC

Enterprise Solutions Competency Center

0308_TA_LT_1000

http://escc.army.mil

ESCC • 6000 6th St., S302 • Ft. Belvoir, VA 22060 • chip.raymond@us.army.mil